2008-01-00

Recent Patterns of Terrorism Prevention in the United Kingdom

Irons, Larry R.

Monterey, California. Naval Postgraduate School

Homeland Security Affairs (January 2008), v.4 no.1

Recent Patterns of Terrorism Prevention in the United Kingdom

Larry R. Irons

INTRODUCTION

The Provisional Irish Republican Army (PIRA) was the basic internal security threat to the United Kingdom over the past 100 years. In particular, more than 3,600 people died during the "Troubles" (1969-1996). However, authorities no longer consider Irish paramilitary organizations the country's major terrorist threat.[1] The major terrorist challenge to the UK today comes from international terrorist groups affiliated with al Qaeda. Until recently, the nexus of the affiliation with al Qaeda was Pakistan and Afghanistan. Recent attacks suggest a nexus with Iraq as well. However, the emergence of a new threat such as al Qaeda does not mean that intelligence analysts' thinking, conditioned to meet one threat, e.g. PIRA, adjusts readily to the new threat.[2] The analysis here highlights this issue in the recent patterns of terrorism prevention in the UK.

Three agencies make up the national intelligence and security services in the UK, The Secret Intelligence Service (MI6) – the nation's external intelligence agency overseen by the foreign secretary; the Government Communications Headquarters (GCHQ) – which develops signals intelligence, also overseen by the foreign secretary; and the Security Service (MI5), which operates under the authority of the home secretary to conduct surveillance operations. Observers often refer to the three services as the Agencies. MI5 has no arrest powers of its own, meaning its ***effectiveness*** in preempting terrorist operations depends largely on collaboration with the Special Branch (SB) of local police forces', especially the Metropolitan Police Department's Special Branch (MPSB).[3]

Following the September 11, 2001 attacks (9/11) in the United States, the government of the UK assumed the consensus opinion that the Agencies had failed to recognize the significance of al Qaeda.[4] As a result, MI5 established the Joint Terrorism Analysis Centre (JTAC). JTAC was hailed as "the most significant structural development within the intelligence community," pooling international terrorism intelligence in one central location "under the direction of one central authority, the director-general of MI5."[5]

Islamic extremists either attempted attacks, or successfully attacked, the UK in the summers of 2005 and 2007. In addition to actual attacks, the Agencies disrupted numerous plots within the UK by terrorist groups over the past few years. The discussion below analyzes patterns in the prevention activities of the intelligence, security, and police services of the UK by examining three terrorist attacks, but principally the most devastating one on July 7, 2005 (7 July) as well as the two most complex preempted plots.

Following William Pelfrey's seminal article on the cycle of preparedness framework,[6] the analysis here uses the Prevention Cube model[7] (see Figure 1) to explore the relationship between terrorist attacks in the UK that occurred since 7 July, and key plots in which authorities successfully intervened to preempt attacks. To do so requires a common framework for analyzing "successful" and "unsuccessful" attack plots. Just as effective collaboration and information sharing provide a basis for recognizing threats,

and deciding whether to intervene to preempt them, so can ineffective collaboration and information sharing result in failure to develop opportunities for preemption.

Pelfrey characterizes the importance of prevention to the Cycle of Preparedness in the following manner: "The Cycle of Preparedness places greater weight on Prevention…It does not carry with it the assumption that there must be an incident as an initiator of the Cycle. Indeed, an organization or jurisdiction must simultaneously prepare for prevention activities, response capacity, and recovery capabilities."[8] The Prevention Cube is a "thinking tool", a heuristic device, useful in analyzing the way prevention principles inform risk management and enable preemption of terrorist threats. It draws from the Cycle of Preparedness framework, yet focuses specifically on prevention, representing the prevention process as a set of steps (front side – Figure 1) that involve preparedness professionals working together and sharing information to recognize threats posed to communities.

Figure 1 – Prevention Cube

Individuals plotting terrorist attacks make strategic choices to develop specific capabilities based on what they see as vulnerable targets. A targeted community can also make choices that lessen its vulnerabilities (top side – Figure 1) and identify the weakness of potential attackers' capabilities. The Prevention Cube exemplifies how key variables of the prevention process relate. Although it implies steps of prevention occur in a sequence, that sequence (front side – Figure 1) doesn't have an exact start or finish, nor do collaboration, information sharing, or threat recognition activities happen in any particular order. The purpose of the prevention process is to manage the risks posed by existing threats and vulnerabilities, and make decisions about how and when to intervene against threats (right side – Figure 1) to protect against them, deter them, or preempt them (top side – Figure 1). Authorities can intervene against threats when the risk posed is in:

1. **Primary Mode**: An intervention to reduce risk when specific threats are unknown but a threat capability, or vulnerability, is recognized.
2. **Secondary Mode**: An intervention to reduce risk after a specific threat is recognized but no immediate threat exists.
3. **Tertiary Mode**: An intervention to reduce, or preempt, a threat that poses a clear-and-present danger.[9]

The following analysis explores several successful and preempted (unsuccessful) terrorist plots in the United Kingdom. We explore the way the Agencies collaborated and shared information to identify threats posed by al Qaeda. Specifically, the analysis herein uses the Prevention Cube as an interpretive resource to analyze recent patterns of terrorism prevention in the United Kingdom. The discussion examines the patterns of collaboration, information sharing, threat recognition, risk management, and decisions

by the Agencies to intervene against a range of terrorist plots. Each section of the analysis focuses on one of the five steps in the Prevention Cube framework relative to specific activities taken by the Agencies to manage the risks posed by al Qaeda to the United Kingdom.

As explained below, the prevention process is not simply a set of linear steps – especially the process of collaborating and sharing information to recognize threats. Prevention often involves cycling through opportunities to recognize threat, gauge risks, and make decisions about intervening. The cycling can occur multiple times and improves in effectiveness when those attempting to prevent terrorist attacks view terrorist organizations, particularly al Qaeda, as networks capable of operating without an explicit command and control hierarchy.[10]

MI5, in particular, missed key opportunities to develop information about the 7 July and 21 July terrorist plots in large part because its risk management strategy failed to use a network conception of terrorist cells and connections between cells. Rather, the available open source information indicates MI5 selected avenues of investigation based largely on a hierarchical model of an investigative target's relationship to foreign al Qaeda operatives or associates. While recognizing the network of relationships underlying a terrorist organization is certainly easier after the fact, failing to use a network conception of terrorist organization against al Qaeda in the prevention process makes successful preemption less likely.[11]

THE CONTEXT

The Agencies are facing an ongoing threat by Islamic extremists as evidenced in the frequency of attacks and ongoing plots in the United Kingdom. The Agencies preempted several attack plots over the past few years. Several attacks occurred as well, though only one actually resulted in a successful execution with lethal consequences. The following analysis examines the patterns of activity common to both types of attack plot.

Preempted Attacks

Details about the fertilizer bomb investigation from 2004, *Operation Crevice*, became available once the trial started in 2006 and after the verdicts in 2007. Operation Crevice is the name given to an investigation into a 2004 plot to build a car bomb using ammonium nitrate fertilizer. At the time, it was the most complex counterterrorism operation ever undertaken in the UK. In the spring of 2007, five men received life sentences for their roles in the plot.[12]

The liquid bomb plot that targeted commercial airlines in 2006 is still under pretrial restriction but salient facts regarding the way authorities disrupted the plot are available as we note below.

Successfully Executed Attacks

By "successfully executed" we mean the attack plot was carried out. Even though the bombs did not explode in two of these three attacks, the plot itself went undiscovered and the attackers were able to execute their operation.

On July 7, 2005 around, 0850, three explosions rocked the London Underground System (hereafter the Tube) and one additional explosion ripped through a London bus in Tavistock Place. The explosions resulted from suicide bomb attacks by Mohammed Siddeque Khan, Hasib Hussein, Shazad Tanweer, and Jermaine Lindsay. The first three

were British nationals of Pakistani descent, born and raised in the United Kingdom. Lindsay was a British national of West Indian Origin and a Muslim convert. All of the bombers on 7 July died in the attack, so investigators developed very little information on the plot from them directly. Khan and Tanweer recorded suicide videos while visiting Pakistan and that fact made al Qaeda involvement evident, as al Qaeda released the videos to the public.[13]

On 21 July 2005, between 1235 and 1305, three additional bomb attempts occurred in the Tube. Six individuals were charged. In July 2007, a jury convicted Yassin Omar, Ramzi Mohammed, Hussain Osman, and Muktar Said Ibrahim, the leader of the plot. The same jury failed to reach a verdict on two others, Manfo Kwaku Asiedu and Adel Yahya. Police developed information regarding the 21 July plot from the defendants as well as other sources. The essential facts relating to the plot became public as the trial proceeded. We discuss them below.

On 29 June 2007, Kafeel Ahmed, Dr Bilal Abdullah, Dr. Mohammed Asha, and Dr Sabeel Ahmed attempted to detonate a car bomb outside a nightclub in London and, after failing to detonate the car bombs, mounted a suicide bomb attack on the Glasgow airport on 30 June. The bomb in the attack on the Glasgow airport also failed to detonate, with Ahmed incurring burns on 90 percent of his body and dying in early August. Bilal Adbullah, Mohammed Asha, and Sabeel Ahmed are awaiting trial. Australian authorities arrested a fourth man, Dr Mohammed Haneef, at the request of the UK. Haneef gave his cell phone's sim card to Kafeel Ahmed for use on a mobile phone used in the attack. The Australian authorities subsequently freed Haneef who returned to his home in India.

The government released two official reports following investigations into the *lethal* attacks on 7 July. One report came from the Intelligence and Security Committee (ISC) of Parliament[14] and the other in a response of the government to the ISC report.[15] Both pointed to several shortcomings in efforts by MI5, the Security Service or domestic spy service in the United Kingdom, as well as the other security agencies, to prevent the attacks.

The reports relied heavily on witnesses, written assessments, and intelligence reports by the Joint Intelligence Committee (JIC) as well as the Joint Terrorism Analysis Centre (JTAC). Yet information developed from the recently concluded trial of the 21 July attackers, as well as developments in the terrorist threat evidenced by the June 2007 attack attempts in London and Glasgow, add fundamentally to our understanding of MI5's failure to recognize the attackers of 7 July and 21 July as operational threats, thereby missing chances to preempt the attacks.

PREVENTION IN PRACTICE

Collaboration

The Prevention Cube treats collaboration as the basic building block of prevention. Though MI5 is most effective when it collaborates with the Special Branch police, the history of collaboration between the two agencies is a challenged one. As Peter Chalk and William Rosenau note, "areas of friction have arisen between the Security Service and local Special Branch police, particularly in instances in which MI5 case officers have moved to centrally sanitize intelligence gathered from covert human sources employed in joint-owned operations."[16]

Prior to the 7 July and 21 July attacks, MI5 recognized the existence of "home-grown" terrorists but gave little credibility to arguments that any operations threatened the UK. The focus prior to 7 July was on plots where key al Qaeda operatives were involved, largely originating from outside the United Kingdom. The 7 July and 21 July bombings refocused attention on the terrorist threat to the UK in several distinct ways. In their examination of the 7 July bombings, British authorities determined a need for more collaboration between MI5 and the Special Branches to help prevent future attacks by home-grown terrorists:

> More needs to be done to improve the way that the Security Service and Special Branches come together in a combined and coherent way to tackle the "home-grown" threat. We welcome steps that are now being taken to achieve this although, given that the 'home-grown' threat had clearly already been recognized, we are concerned that more was not done sooner.[17]

The overall shortcomings in effective collaboration before 7 July reached across the security and intelligence services, including the Security Service (MI5), the Secret Intelligence Service (SIS) or MI6, and the Government Communications Headquarters (GCHQ). In particular, prior to 2005, the SIS provided insufficient intelligence coverage on countries like Pakistan where al Qaeda still maintains training camps. At the same time, the focus of MI5 investigations was largely on plots involving direct connections to al Qaeda operatives in Pakistan.

All the terrorist attacks, except the most recent one, and the two disrupted plots, involved al Qaeda affiliates in Pakistan supplying key training and planning resources to those involved in the plots. Manfo Kwaku Asiedu, charged in the 21 July plot testified that Ibrahim, the leader of the 21 July attack, and Khan, the leader of the 7 July attack, were in Pakistan at the same time and planned the attacks there.[18] In addition, Mohammed Junaid Babar, who was arrested in New York for planning attacks on financial institutions on the U.S. east coast, testified as part of a plea bargain that Khan traveled to the Pakistan border near Afghanistan in 2003 for terrorism training.[19]

The relationship between the U.K. and Pakistan is a complex one with a rich history. More than 400,000 people travel between the two countries each year. The Agencies do not know how many of those people continue their journey to Afghanistan or the tribal areas of Pakistan. Estimates are that as many as 4,000 Islamic extremists have attended camps in Afghanistan and returned.[20] However, the pattern of attacks and disrupted plots indicates an overall coordination between Islamic extremists, al Qaeda or its affiliates, in Pakistan, and the home-grown terrorists of the UK. *The pattern indicates an ongoing ability of al Qaeda to act as a network providing training and planning resources as well as an ideological source of motivation, without the exposure of a command and control hierarchy.*[21]

It is now clear MI5 knew about Khan well prior to 7 July, but failed to make key connections related to his activities. In early 2004, detainees from outside the UK referred to a man during questioning, known only through pseudonyms, who they claimed had traveled to Pakistan in 2003 seeking a meeting with al Qaeda leaders. MI5 tried to establish the man's identity but failed. As it turned out, Khan was the man. One of the detainees after 7 July identified a photograph taken of Khan at one of the meetings in 2004. Khan in fact did travel to Pakistan in 2003 and spent time there again with Tanweer from November 2004 to February 2005. Apparently, authorities did not

show the photograph to the detainee until after the 7 July attacks. The detainee then identified the person in the photograph as Khan.

In other words, MI5 did not pursue specific opportunities to develop intelligence about Khan and Tanweer. In instances where it did develop intelligence on Khan from other ongoing investigations, MI5 did not pursue those opportunities. For example, MI5 considered Khan and Tanweer peripheral to the Operation Crevice investigation. *The judgment was accurate in quantitative terms, but telling and consequential in analytic terms.*

INFORMATION SHARING: THE UNKNOWN AS AN INFORMATION SOURCE

Operation Crevice resulted from information provided by an employee at a rental-storage business where the terrorist cell was storing the fertilizer for a bomb. He became suspicious and contacted the authorities. Similarly, following the 7 July and 21 July attacks, MI5 received a tip from a member of the Muslim community regarding an acquaintance thought to be involved in terrorist-related activity. MI5 started investigating the individual and, over time, the liquid bomb plot was uncovered. In fact, the investigators substituted a different chemical for the fertilizer during Operation Crevice, without the plotters' discovering the switch. Applying the Prevention Cube (top side – Figure 1) suggests that this countermeasure was essentially a step to **Protect** against the threat capability posed by the plot even if the plotters executed the plan. Essentially, such a protective measure permitted MI5 to extend its investigation of a recognized **Secondary Mode** risk (right side – Figure 1) rather than intervene sooner to **Preempt** the threat posing the risk. Consider the following summary of Operation Crevice in the context of the Prevention Cube:

> In many ways both the primary and secondary modes are focused on making good use of time available to prevent and mitigate, rather than just respond to risk....After initial surveillance it was decided the plotters were still in the process of gathering bomb elements. The risk was still in secondary mode. As a result, surveillance continued in order to identify all the plotters, their sources of support, and other operational details. The arrest was timed to ensure the risk did not enter the tertiary mode, but it was delayed to maximize the options available in the secondary mode.[22]

The UK authorities also preempted the liquid bomb plot in August 2006 after months of intensive surveillance involving British, American, and Pakistani intelligence agencies. In other words, in the two most noted British successes in disrupting terrorist attacks, the prevention of the plots began with human intelligence from the public. Authorities knew the source of the information that initiated or bolstered the investigation.

One of the major lessons learned from 7 July and 21 July is that opportunities to investigate the unknowns relating to a case require proactive intelligence practices. *What is not known must be explored in order to make informed decisions about what needs to be learned.* As the ISC report noted:*

> ...the main lesson learned from the July attacks was the need to get into "the unknowns" – to find ways of broadening coverage to pick up currently unknown terrorist activity or plots. We were told that Security Service and police efforts prior to July were focused on following up known intelligence leads in the UK,

> arising either out of other terrorist investigations, from GCHQ or the SIS, or from foreign intelligence reporting. Resources were fully consumed with the pursuit of existing leads and there was little capacity to look beyond to see where other threats might be developing. Steps are now being taken to develop a more proactive approach to identifying threats in the UK, first through *** and second through closer working with the police at the local level.[23]
>
> * The asterisks represent redaction

The 7 July and 21 July attacks heightened recognition that much remains unknown about the ideologically motivated Islamist activity at the local level in the UK, and its relationship to al Qaeda affiliates in Pakistan. The focus since the attacks is on building a "rich picture" of local extremists using the police, MI5, and the police Special Branches working closely together. The Special Branches are a part of the police forces but also recruit and run agents for MI5. As noted previously, the relationship between the two has been difficult historically.

The local constabulary funds the Special Branches and, in the past, that caused significant differences in their effectiveness from locale to locale. Since 7 July, an emphasis on national standards for the Special Branches is evident. The ISC report concludes:

> Special branches continue to vary in size and competence.... There is, moreover, no specific requirement for their Special Branches to meet a certain standard in the counter-terrorism work they do conduct in support of the Security Service.... The value of closer joint working between the Security Service and the police on a more local level is one of the key lessons to arise from the July attacks.... Where there may in the past have been a reluctance to give bad news and upset good relations, there appears, rightly, to be more determination post-July for problems or areas of weakness to be identified and resolved.[24]

The Terrorism Act of 2006 made it a criminal offense to directly or indirectly encourage the commission, preparation, or instigation of acts of terrorism or to disseminate terrorist publications, including statements or publications glorifying terrorism. The Act also broadened the legal basis for proscribing organizations that promote or encourage terrorism. Therefore, the local police and the Special Branches, as well as MI5, now possess extensive legal authority to gather intelligence from extremist groups and intervene using a variety of state powers, including extending the period of pre-charge detention from fourteen to twenty-eight days.[25] Whether these new powers will make a difference in MI5's decisions about investigating individuals who are peripheral to an ongoing investigation into high priority targets is an important question.

Indeed, the 2007 bomb attacks in London on 29 June and Glasgow on 30 June point to continuing problems regarding MI5's ability to recognize information with significant intelligence value. Bilal Abdulla and Mohammed Asha, who lived almost 300 miles apart, kept in regular contact, with their discussions intercepted by GCHQ and drawing the attention of MI5. However, the intelligence point of view on missed opportunities to learn about *unknowns* turns the criticism of failed assessment on its head. An intelligence source was quoted saying,

> The fact that these two had already been flagged up, albeit in a very minor capacity, is a great relief because it shows that we are doing our job. The nightmare scenario is a case when we get hold of someone or learn about

> someone who has never before crossed our path. Then you have to start from scratch.[26]

The point echoes the position taken by MI5 about its failure to give Khan and Tanweer higher priority as investigation targets before 7 July.

MI5 noted that the links between Khan and Tanweer and the fertilizer bomb plotters represented less than 0.1 percent of all the links on record for Operation Crevice. Nevertheless, the ISC report's point about exploring the *unknowns* in an investigation implies that the total *quantity* of links is not sufficient for determining whether an opportunity to investigate a peripheral target is reasonable. *The context of the links means a lot as well.* MI5 surveillance also linked Khan and Tanweer to the leader of the fertilizer bomb plot, Omar Khyam. That fact meant as much to Khan and Tanweer's intelligence value as how many links existed between them and the fertilizer bomb plotters as a group. After all, Khyam was the *known* leader of the fertilizer bomb plot.

A brief discussion of two key concepts from social network analysis (SNA) will clarify the point regarding the investigation of unknowns and the risk management strategy used by the Agencies. In its most basic form, social network analysis distinguishes between two types of centrality measures that appear relevant to the point, specifically *degree centrality* and *betweenness centrality*.[27]

Degree Centrality

Degree centrality is broken down in SNA according to *in-degree centrality* and *out-degree centrality*. The former refers to the number of incoming links an individual has in a given relationship. The latter refers to the number of outgoing links an individual has in a given relationship. A social network with high degrees of both is a highly cohesive network for all members, resembling what John Arquilla and David Ronfeldt referred to as an "all-channel" network (Figure 2) in their analysis of Netwar.[28]

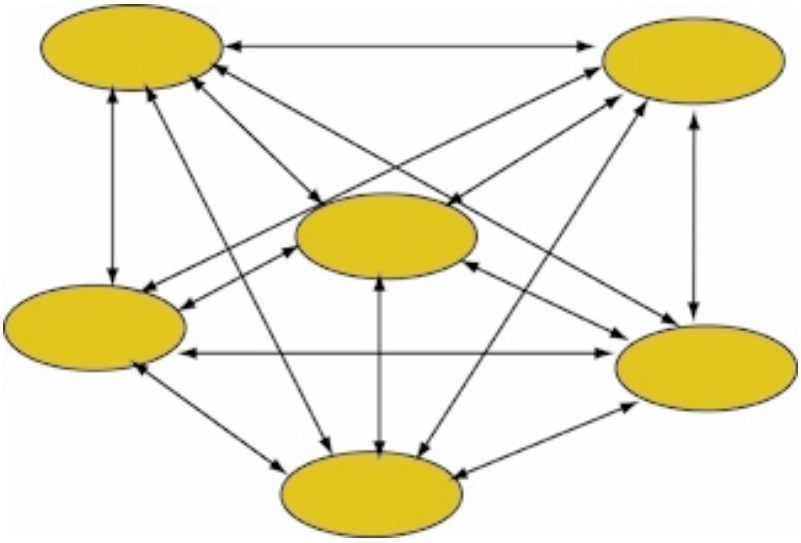

Figure 2

Differences between in-degree and out-degree centrality occur in networks where some members are more connected to the network than others. Some members exert more influence on the network by having high out-degree centrality (e.g. Khan and Tanweer in Figure 3), whereas the network influences others who have high in-degree centrality (e.g. Lindsay and Hussein in Figure 3).[29]

Betweenness Centrality

MI5's point that it decided not to continue surveillance of Khan and Tanweer because the quantity of Khan and Tanweer's links to the fertilizer bomb plotters targeted in Operation Crevice were less than 0.1 percent of the total links fails to take into account the betweenness centrality of Khyam. Betweenness centrality refers to relationships where one individual provides the most direct connection between two or more groups. These individuals *bridge* networks, or subnetworks.[30] In the case of Khan and Tanweer, Khyam was likely serving a *liaison* role rather than a broker role (Figure 3), meaning his betweenness was not likely critical to their plot but was *indicative* of Khan and Tanweer's intelligence value. MI5 recognized the first point but apparently missed the second. Khan and Tanweer's connection to Khyam was an unknown that merited further investigation.

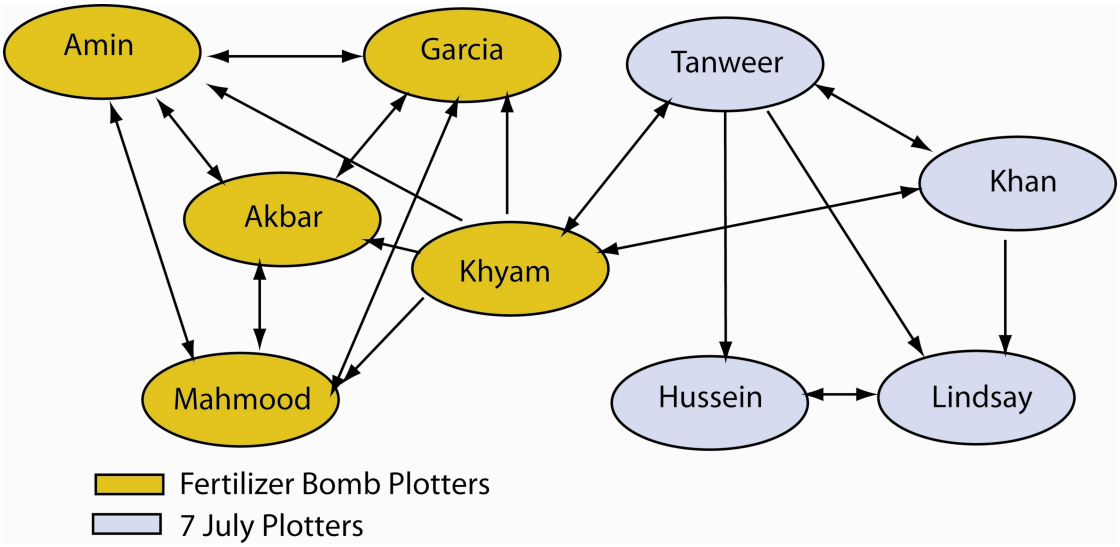

Figure 3

Links existed between Khan and Tanweer to other members of the fertilizer bomb plot since MI5 observed them driving with the group. However, the open source intelligence indicates their connections with Khyam were denser, more frequent. Given Khyam's leadership in the fertilizer bomb plot, of which authorities were aware, the repeated links MI5 observed between Khan and Tanweer to Khyam were significant when compared to their links to other members of the plot.

THREAT RECOGNITION

Failing to recognize the threat that British nationals were capable of and likely to engage in suicide bombing was one of the major shortcomings of British authorities, specifically MI5, before 7 July 2005. This was despite the fact that Richard Reid, who tried to detonate a shoe bomb on an American Airlines flight to the United States, was a British citizen. The ISC report also states that Omar Sharif and Asif Hanif, two young British Muslims, tried to execute a suicide bomb attack against a bar in Tel Aviv in 2003. (The BBC corrected the point, noting that one of the bombers set off the device killing three people, while the other detonated later to avoid capture.)

The Agencies did not adequately appreciate the threat posed by home-grown terrorists:

> We remain concerned that across the whole of the counter-terrorism community the development of the home-grown threat and the radicalisation of British citizens were not fully understood or applied to strategic thinking.[31]

The Prevention Cube is helpful in sorting out the issues involved and providing a coherent interpretation of the developments. The threat from British nationals, willing to plan and execute suicide bomb attacks against iconic targets like the Tube, was in fact a recognized **Primary Mode** risk by the security agencies before 7 July.

In other words, the Agencies recognized the Tube as a likely target for terrorists given the frequency of al Qaeda inspired terrorist attacks on mass transit, and the Madrid bombings of 2004. Yet, the protective measures taken mostly aimed to deter terrorists from attacking who were not engaging in suicide bombing. The video surveillance system in the Tube is one of the most extensive in the world. It was highly effective in permitting the authorities to determine who the suicide bombers were after the fact, but ineffective in deterring them from the attack.

To some extent, *one could reasonably surmise that the strategy and tactics of the PIRA, with its focus on volunteer safety, still dominated the counterterrorism thinking of* the Agencies *on deterrence before 7 July*.

The Agencies had intelligence from their own investigations and third parties that pointed in at least seven ways to the 7 July leader, Khan, as a higher priority figure than thought at the time.

1. In his book, *The One Percent Doctrine*, Ron Suskind contends that Khan was planning to visit the United States in February 2003.[32] Khan had done so three times since 2001. The CIA contacted the FBI to ask for a coordinated effort to track Khan's movements and contacts. An NSA surveillance program recorded Khan's communication with other Islamic extremists in the United States, with clear indications of an interest in mounting attacks in the U.S. Yet, according to Ron Suskind, the FBI and the CIA were unable to work out their differences over which agency would accept responsibility for Khan's activities if he initiated an attack while in the country. In other words, neither agency wanted the responsibility of managing a **Secondary Mode** risk. As a result, the FBI placed Khan on a "no-fly" list the night before he was supposed to catch a flight to the United States. *U.S. authorities reportedly told British officials of Khan's plans and the decision to place him on a "no-fly" list and forwarded a detailed file*.[33]

2. Khan and Tanweer met with the leader of the fertilizer bomb plot, Omar Khyam, at least five times in the weeks of the final planning stages of the plot. Khan and Tanweer were among a group of men meeting, where others at the meeting were under MI5 surveillance in 2004. MI5 considered Khayam a high level, or "essential," target. "Essential" targets are highest priority with the most immediate claim on resources, with "desirable" targets second, and "other" last. The distinctions depend on the degree of affiliation to al Qaeda that the target is suspected of possessing. The meetings in 2004 were associated with the ongoing investigation in Operation Crevice.
3. Khan and Tanweer were among fifty-five individuals considered worthy of follow up after the charges were filed against the fertilizer bomb plotters. Fifteen were considered essential to follow up, and forty were considered desirable. Khan and Tanweer were in the latter group.
4. MI5 had also bugged a conversation between Khan and Omar Khyam, leader of the "fertilizer bomb" terrorists arrested as part of Operation Crevice. Court transcripts showed the two were discussing going to Pakistan to train as well as how to commit financial fraud to support their activities.[34]
5. Khan and Tanweer were followed while driving with the fertilizer bomb plotters and took anti-surveillance precautions. The Agencies followed the car that Khan ultimately drove to his home.
6. In March 2004, the authorities checked the ownership of the vehicle Khan drove and found it was registered to his wife. Two months later, another ownership check showed it registered to Khan under a different address.
7. Clear evidence from surveillance tapes showed Khan was planning on acquiring terrorism training overseas and discussing specific attack plans.

The ISC report indicates that, at the time, MI5's assessment suggested Khan and Tanweer's focus was training and insurgency operations in Pakistan, and schemes to defraud financial institutions. However, we now know that MI5 did not give the ISC a full accounting of how much it knew about Khan in particular.

More recently, Shadow Home Secretary David Davis questioned the Home Secretary, John Reid about MI5's failure to disclose all the relevant information.

> It seems that MI5 taped Mohammad Sidique Khan talking about his wish to fight in the jihad and saying his goodbyes to his family -- a clear indication that he was intending a suicide mission....[H]e was known to have attended late-stage discussions on planning another major terror attack. Again, I ask the Home Secretary whether that is true.[35]

Mr. Reid indicated the question was relevant but declined to answer it. We now know Khan was a threat posing a **Secondary Mode** risk that developed over a period from 2003 while he organized the other three members for the 7 July attacks. Additionally, the ISC reports that the intelligence services now believe Khan met with al Qaeda during his visit to Pakistan and Afghanistan in 2003. *A **Secondary Mode** risk occurs when there are early signals of a specific threat emerging*. As noted above, there were at least seven points of intelligence indicating that Khan posed a terrorist threat.

MI5 made a similar series of omissions and judgments about the leader of the unsuccessful 21 July bomb attacks, Muktar Said Ibrahim.

1. Ibrahim was photographed in May 2004 at a jihadi training camp in the north-west of England. As the Times noted, Ibrahim aroused suspicion from his association with Rauf Mohammed who actively supported the insurgency in Iraq. Mohammed drove Ibrahim and two traveling companions to the airport in December 2004 as they flew to Pakistan for terrorist training.[36]
2. The association with Mohammed resulted in Ibrahim and his traveling companions being questioned at the airport by Special Branch police.
3. Ibrahim was arrested at an extremist bookstall in London for scuffling with a policeman over extremist literature Ibrahim was distributing, and an outstanding warrant for his arrest was issued for failing to show in court on a public order offense.
4. Ibrahim was given a British passport and allowed to leave the country despite a prior criminal record and an outstanding warrant. Officers found a large amount of cash, mountain gear, and a first-aid manual with marked passages on treating gunshot wounds. Ibrahim was permitted to leave after explaining he was going to Pakistan to attend a wedding.
5. MI5 received an alert upon Ibrahim's return to the UK in early 2005. It considered him a low-key target and missed the fact that he was recruiting a cell of suicide bombers.

On July 21, 2005, Ibrahim attempted to blow up the No. 26 bus. His accomplices, Yassin Omar, Hussein Osman, and Ramzi Mohammed also failed in their bomb attempts. Luckily, none of the devices exploded.

*A **Tertiary Mode** risk poses imminent harm from a recognized, specific threat.* MI5 now believes Khan and Tanweer underwent operational training while in Pakistan. Moreover, leading up to the attack, during the tertiary risk period, Khan was in contact on over 200 calls from his phone to various phone booths and mobile phones in Pakistan. Interestingly, the ISC report did not criticize the Government Communications Headquarters (GCHQ) for failing to consider the pattern of contacts significant. Although the ISC report did not spell out exactly how the security service plans to go about it, the future focus is on an increasingly proactive strategy using a network analysis approach.*

> Security Service and police efforts prior to July were focused on following up known intelligence leads in the UK, arising either out of other terrorist investigations, from GCHQ or the SIS, or from foreign intelligence reporting. Resources were fully consumed with the pursuit of existing leads and there was little capacity to look beyond to see where other threats might be developing. Steps are now being taken to develop a more proactive approach to identifying threats in the UK, first through *** and second through closer working with the police at the local level. The potential value of *** and *** as a means for identifying new threats has been highlighted to the Committee. The fact that the 7 July group was in contact with others under Security Service investigation has emphasised the potential for new threats to be identified through the examination of information and contact networks relating to existing targets.

> Greater capacity to *** to generate new leads is being developed within the Security Service.[37]
>
> * The asterisks represent redaction

As part of the overall proactive strategy, a discussion of whether to change the law and allow authorities to use intercepted communication as evidence is underway. Drawing from the U.S. experience, the director of public prosecutions contends that using intercepts as evidence will increase terrorism prosecutions and drive up the percent of guilty pleas, making control orders less necessary.[38] The Prevention of Terrorism Act of 2005 authorized the secretary of state, under judicial oversight, to issue a control order to place one or more obligations on individuals to prevent, restrict, or disrupt their involvement in terrorism-related activity. The obligations can include curfews, restrictions on use of communications equipment, restrictions on personal associations with others, and travel restrictions.[39]

Some observers, citing patterns of prosecution in the United States, contend that allowing intercepts as evidence will decrease the need to use control orders by increasing guilty pleas, thereby allowing more prosecutions. [40] The Baroness Scotland of Asthal, Patricia Janet Scotland, a barrister and attorney general for England and Wales, a ministerial position in the British Government, disagrees with the contention that using intercepts as evidence will increase prosecutions. On the contrary, Baroness Scotland contends that,

> It is sometimes argued that if only we could produce intercept evidence against terrorists we would be able to lock more of them up and avoid measures such as control orders. That is simply untrue. The last review concluded that there would be, I emphasize, very limited utility against terrorists.[41]

It is unclear how the policy issue of using intercepts as evidence will develop. Allowing intercepts to qualify as evidence raises a range of issues that come from long-standing traditions involving the relationship of MI5 to the Special Branches and the local constabulary. Allowing intercepted communication to count as evidence at trial might well result in the UK preempting threats earlier in their development, effectively reducing *the Agencies*' timeframe for managing **Secondary Mode** risks.

RISK MANAGEMENT

One of the inherent challenges of prevention is the impossibility of preventing all adverse events. Judgments made at specific points in time influence what threats authorities recognize, and the conceptual framework in which they assess risk. The most important thing is to base those judgments on good information and a full recognition of the threats, *known* and, to the extent possible, *unknown*. Allowing previous assessments of a target's priority to determine how new opportunities, i.e. linkages, to investigate the target are managed tends to preclude, or at least minimize, a concern with the unknown. The 7 July attackers benefited from that overall counterterrorism strategy, as did those involved in the 21 July attack.

In addition to MI5 hierarchically organizing investigative targets according to whether they are "essential," "desirable," or "other," the Joint Terrorism Analysis Centre (JTAC) also introduced an analogous three-tier, hierarchical model in early 2005 regarding the degrees of connection between targets and al Qaeda leadership:

Tier 1 described individuals or networks thought to have direct links to al Qaeda.

Tier 2 described individuals or networks loosely affiliated with al Qaeda.

Tier 3 described individuals or networks inspired by al Qaeda ideology.

In May 2005, JTAC considered the majority of its focus on individuals and groups from Tiers 2 and 3 only loosely affiliated to al Qaeda or entirely separate (albeit with shared ideological beliefs). JTAC considered the group responsible for the Madrid bombings in 2004 a Tier 3 group.

The Agencies used tiered designations to prioritize resource expenditure, but none of these hierarchies took into account the relevance of unknown factors. If investigators had kept in mind a network conception of al Qaeda organization, rather than directing activities through hierarchical assessments driven by what was "known," different decisions might have led them to discover what Khan and Tanweer were up to. The ISC report reaches the same conclusion in a more indirect way:

> The chances of identifying attack planning and of preventing the 7 July attacks might have been greater had different investigative decisions been taken in 2003–2005. Nonetheless, we conclude that, in light of the other priority investigations being conducted and the limitations on Security Service resources, the decisions not to give greater investigative priority to these two individuals were understandable.[42]

In other words, the ISC and government reports agree that scarcity of resources, rather than mistaken decisions about risk, was the main reason MI5 did not investigate the two men, though it indicates that the investigative decisions made during the crucial time period between 2003 and 2005 could have affected the outcome.

MI5 allocated resources to investigate Khan and Tanweer late in 2004, probably because they were among the fifty-five individuals deemed to merit follow up after Operation Crevice. However, MI5 soon diverted the funding to investigations considered higher priority. Yet, a number of experts question whether the ISC report's focus on resources was adequate to develop an understanding of how MI5 decision making went wrong.

> A number of experts are increasingly frustrated by the concentration on the numbers game in the aftermath of the attacks. "To say that the intelligence services are exonerated and were hampered by lack of resources really says nothing of substance," said Mike Smith, an intelligence expert at King's College, London. "One can have vast resources and still make mistakes, miss out what is going on and fail to connect the dots - think of the failure of the vast intelligence resources in the US to anticipate the 9/11 attacks." The assessment of Anthony Glees, a renowned intelligence-watcher from Brunel University, is even more emphatic. He told Scotland on Sunday: "MI5 seems to have wanted it both ways: first of all punters like myself learned from our sources that the problem had been one of 'resources'. But just a few days ago, *I was told that resources were not the problem - the problem had been one of failed assessment*. If it had been 'resources' it would have prompted the next question: 'Did you ask Gordon Brown for more cash?' But I am told they did not ask for more cash in 2005 because they were more or less satisfied with what they had."[43]

Regardless of MI5's view of its need for resources in 2005, the service has since increased its overall staff significantly. Yet MI5's methods for establishing who is a high priority target, and who isn't, were only indirectly assessed by the ISC report.

Nevertheless, the decision not to give Khan and Tanweer greater priority at the time points to a failure on the part of investigators' assessment of their importance. *The investigations failed to recognize that individuals connected on multiple occasions with other, higher priority, individuals under active surveillance present opportunities to learn about unknown threats, i.e. nodes in a network, that increase the lower priority target's intelligence value.*

It is reasonable to assume that the Agencies' experience with PIRA informed efforts against al Qaeda since, even after PIRA restructured itself from a hierarchical, military style organization to a group of loosely-coupled cells in the 1980s, high profile attacks on UK government officials that required special teams were still typically controlled directly by the GHC [General Headquarters].[44] Similarly, al Qaeda operational leaders based in Afghanistan largely directed the attacks on 9/11.[45] The 7 July attack demonstrated that the kind of direct coordination informing the counterterrorism strategy of the Agencies was insufficient to detect the emerging threat from home-grown terrorist attacks by Islamic extremists.

It appears that authorities now recognize the importance of thinking in network analysis terms as well as hierarchical priority structures when considering the relative importance of targets in a terrorism investigation. MI5 still contends it cannot follow up 100 percent of the individuals it comes across that are peripheral to an investigation, but security sources are quoted saying that figures peripheral to investigations are constantly reassessed currently.[46] As we noted above, individuals considered peripheral, yet connected with leaders of other ongoing plots, offer increased intelligence value since those leaders' betweenness status can indicate a broker or liaison role.

INTERVENTION

MI5 did not develop intelligence to allow it to make a decision to intervene against the attackers of 7 July or 21 July. The risk-management strategy largely precluded development of intervention opportunities. The ISC and government reports contend that, if more resources had been in place, authorities might have had more information to share, leading to better threat recognition, and a risk-management decision that was more in line with the actual threat. The result might have been an opportunity to intervene.

> The story of what was known about the 7 July group prior to July indicates that if more resources had been in place sooner the chances of preventing the July attacks could have increased. Greater coverage in Pakistan, or more resources generally in the UK, might have alerted the Agencies to the intentions of the 7 July group.[47]

Our analysis indicates that the experience of dealing with PIRA conditioned the risk management strategy the Agencies used to investigate threats posed by al Qaeda. In the case of PIRA, a hierarchical command structure remained in control for strategic attacks on members of the UK government, even after PIRA restructured itself into operational cells. Al Qaeda operations in the UK appear to follow a different pattern.

CONCLUSIONS

This article used the Prevention Cube to identify patterns of terrorism prevention in the United Kingdom since 2004. It discussed successful attack plots and preempted attack plots using the key concepts of the Prevention Cube to think through the assumptions made by the Agencies in the UK regarding the risks posed by the terrorist threat of al Qaeda.

The discussion suggested that the experience with PIRA conditioned the Agencies in the UK to think hierarchically about risks posed by terrorist threats. A different risk management strategy informed by social network analysis could have affected the assessments made in Operation Crevice regarding which individuals to pursue on the periphery of those investigations. Khan and Tanweer, though peripheral to the fertilizer bomb plot, were key leaders in the 7 July terrorist attack.

As a heuristic device, the Prevention Cube does not predict the conditions under which collaboration, information sharing, or threat recognition explain the success of a particular risk management strategy or intervention decision. Rather, the Prevention Cube provides an exemplar for guiding risk management. It informs an adaptive strategy for efforts to collaborate, share information, and recognize threats in each decision to intervene to protect, deter, or preempt risks posed.

Larry Irons received his PhD in sociology from Washington University in St. Louis where he was a university fellow. He is a senior fellow with the National Institute for Strategic Preparedness, a learning architect with Teleologic Learning Company, and an adjunct assistant professor of sociology at the University of Missouri – St. Louis. He is a coauthor, with Craig Baldwin and Philip Palin, of Catastrophe Preparation and Prevention for Law Enforcement Professionals *(McGraw-Hill Higher Education, 2008) and* Catastrophe Preparation and Prevention for Fire Service Professionals *(McGraw-Hill Higher Education, 2008).*

The author expresses his appreciation to the anonymous reviewers of *Homeland Security Affairs*, and for the comments offered by Philip Palin and Craig Baldwin.

---

[1] Peter Chalk and William Rosenau, *Confronting the "Enemy Within": Security Intelligence, the Police, and Counterterrorism in Four Democracies* (RAND Corporation, 2004) http://www.rand.org/pubs/monographs/MG100/

[2] Richard J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, D.C.: Center for the Study of Intelligence, CIA, 1999). Heuer observes that, "it takes more information, and more unambiguous information, to recognize an unexpected phenomenon than an expected one" (p. 8), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf

[3] Chalk and Rosenau, *Confronting the "Enemy Within*," 52-55.

[4] Bradley W. C. Bamford, "The United Kingdom's 'War Against Terrorism'," *Terrorism and Political Violence* 16, no. 4(2004): 737-756.

[5] Ibid, 744.

[6] William V. Pelfrey, "The Cycle of Preparedness: Establishing a Framework to Prepare for Terrorist Threats," *Journal of Homeland Security and Emergency Management* 2 no. 1 (2005), http://www.bepress.com/jhsem/vol2/iss1/5

[7] The Prevention Cube is a tool for practicing principles of prevention that originated with William V. Pelfrey, PhD. The tool was conceived by Christopher Bellavita, Philip Palin, and William Pelfrey. For an overview of the Prevention Cube see Craig Baldwin, Larry Irons, and Philip J. Palin, *Catastrophe Preparation and Prevention for Law Enforcement Professionals* (New York: McGraw Hill Higher Education, 2008).

[8] Pelfrey, "The Cycle of Preparedness," 6.

[9] Baldwin, Irons, and Palin, *Catastrophe Preparation*, 118. These categories of primary mode, secondary mode, and tertiary mode risk represent timeframes within which intervention decisions are made against the threat capability of terrorists. The categories are drawn from the medical model of disease prevention. They are also used in the criminological literature in relation to crime prevention. This article uses the categories of primary, secondary, and tertiary risk to organize thinking about how to manage risk by intervening against terrorist threat capabilities, or lessening target vulnerabilities. The same categories of risk are useful in thinking about interventions against natural and accidental threats.

[10] Hoffman pointed to this characteristic of al Qaeda's network organization in testimony before the Senate Foreign Relations Committee on July 18, 2006. He noted: "The al Qaeda of today combines, as it always has, both a 'bottom up' approach – encouraging independent thought and action from low (or lower-) level operatives – and a 'top down' one – issuing orders and still coordinating a far-flung terrorist enterprise with both highly synchronized and autonomous moving parts;" Bruce Hoffman, "Islam and the West: Searching for Common Ground," *Testimony before the Senate Foreign Relations Committee on July 18, 2006*, http://www.rand.org/pubs/testimonies/2006/RAND_CT263.pdf One of the first to note this network organization characterizing al Qaeda was Rohan Gunaratna, *Inside Al Qaeda* (New York: Berkley Books, 2002).

[11] The assessment offered by van Meter in 2001 remains relevant to the current situation. "Following the 11 September attacks, one would have thought that the concept of pyramidal hierarchical command structures for illicit adversary social networks, particularly for those of Islamic extremists, would have lived out its overextended life. Indeed, both the media and officials, including the Pentagon, have recently called on the social network analysis community for possible contributions in understanding — and fighting or dismantling — such networks. But official thinking has not changed that quickly…it was official thinking about those groups or networks which was hierarchically structured, and in a very rigid manner." Kari M.Van Meter, "Terrorists/Liberators: Researching and dealing with adversary social networks," *Connections* 24, no. 3 (2001): 66-78, http://www.insna.org/Connections-Web/Volume24-3/Karl.van.Meter.web.pdf

[12] "Five get life over UK bomb plot," *BBC News,* April 30, 2007, http://news.bbc.co.uk/2/hi/uk_news/6195914.stm

[13] An overview of these "martyrdom" videos is available in Hoffman's testimony before the Senate Foreign Relations Committee on July 18, 2006. Hoffman, op. cit., 11-14.

[14] *Intelligence and Security Committee Report into the London Terrorist Attacks on 7 July 2005,* 2006, http://www.libertysecurity.org/IMG/pdf/isc_7july_report.pdf

[15] *Government Response to the Intelligence and Security Committee's Report into the London Terrorist Attacks on 7 July 2005*. 2006, http://www.cabinetoffice.gov.uk/publications/reports/intelligence/govres_7july.pdf

[16] Chalk and Rosenau, *Confronting the "Enemy Within*," 52-53.

[17] *Intelligence and Security Committee Report,* 38.

[18] Gordon Rayner and David Williams, "Bombers on benefits," *Daily Mail*. July 9, 2007.

[19] Sebastion Rotella, "British Terrorism Case Parallels Others," *Los Angeles Times*, September 1, 2006.

[20] Ben Leapman, "4,000 trained at Afghan terror camps and returned to UK," *The Sunday Telegraph,* July 15, 2007.

[21] Hoffman, *Testimony*, 10-11.

[22] Baldwin, Irons, and Palin, *Catastrophe Preparation*, 122-123.

[23] *Intelligence and Security Committee Report,* 35-36.

[24] Ibid., 37.

[25] *Countering International Terrorism: The United Kingdom's Strategy*, July 2006. Presented to the Parliament by the Prime Minister and the Secretary of State for the Home Department by Command of Her Majesty, http://www.intelligence.gov.uk/upload/assets/www.intelligence.gov.uk/countering.pdf

[26] Richard Elias, "From Baghdad with Hate," *Scotland on Sunday*, July 8, 2007.

[27] Rob Cross and Andrew Parker, Andrew, *The Hidden Power of Social Networks* (Boston: Harvard Business School Press, 2004).

[28] John Arquilla and David Ronfeldt, *The Advent of Netwar* (Santa Monica, CA: RAND, 1996), http://www.rand.org/pubs/monograph_reports/MR789/index.html We are not here claiming to do a social network analysis of the fertilizer bomb and 7 July plots. An example of how to do such an analysis for the 9/11 attacks was offered in Krebs, Valdis E. Krebs, "Uncloaking Terrorist Networks," *First Monday* 7, no. 4 (2002), http://www.firstmonday.org/issues/issue7_4/krebs/. Krebs notes that any measure of centrality in a network is extremely sensitive to unknown connections that are discovered. Additionally, "Conspirators don't form many ties outside of their immediate cluster and often minimize the activation of existing ties inside the network. Strong ties between prior contacts, which were frequently formed years ago in school and training camps, keep the cells linked. Yet, unlike normal social networks, these strong ties remain mostly dormant and therefore hidden to outsiders." We don't attempt to quantify the variations in connection existing between the various members of the fertilizer bomb plot. Rather, our concern is to represent the key position of Khyam relative to the 7 July plotters when a network concept is used to analyze the fertilizer bomb and 7 July plots.

[29] Cross and Parker, *Hidden Power*, 157.

[30] Ibid., 157.

[31] *Intelligence and Security Committee Report*, 43.

[32] Ron Suskind, *The One Percent Doctrine* (New York: Simon & Schuster, 2006).

[33] Daniel McGrory, "U.S. 'issued alert' on 7/7 bomber in 2003," *TimesOnLine*, June 19, 2006, http://www.timesonline.co.uk/tol/news/uk/crime/article676305.ece

[34] Raymond Whitaker, Paul Lashmar, and Andrew Buncombe, "Al-Qa'ida's voice threatens once more – but what control does he have over atrocities in Britain?" *The Independent*, August 12, 2007, http://news.independent.co.uk/uk/crime/article2771025.ece

[35] "MI5 hid evidence on Tube bombing," *The Australian*, May 15, 2006, http://www.theaustralian.news.com.au/story/0,20867,19134121-2703,00.html

[36] Sean O'Neill and Michael Evans, "How MI5 left ringleader free to acquire recruits and explosives," *The Times*, July 11, 2007.

[37] *Intelligence and Security Committee Report,* 36.

[38] Joint Committee on Human Rights, *Counter-Terrorism Policy and Human Rights: 28 days, intercept and post-charge questioning*, July 30, 2007, http://www.publications.parliament.uk/pa/jt200607/jtselect/jtrights/157/157.pdf

[39] *Countering International Terrorism*, 19.

[40] Of particular significance are the recent discussions in the United States on developing an analog capability in the FBI to the intelligence analysis and case officer approach of MI5. See, for example, James Burch, "A Domestic Intelligence Agency for the United States? A Comparative Analysis of Domestic Intelligence Agencies and Their Implications for Homeland Security," *Homeland Security Affairs* III, no. 2 (2007). Also see, John Solomon, "FBI Reorganizes Effort to Uncover Terror Groups' Global Ties," *Washington Post*, September 26, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/25/AR2007092502291_pf.html

[41] *Counter-Terrorism Policy and Human Rights*, 36.

[42] *Intelligence and Security Committee Report,* 16.

[43] Brian Brady, "Lessons still not learned," *Scotsman.com*, May 14, 2006, http://news.scotsman.com/uk.cfm?id=720032006

[44] Brian A. Jackson, John C. Baker, Kim Cragin, John Parachini, Horacio R.Trujillo, and Peter Chalk, *Aptitude for Destruction Volume 2: Case Studies of Organizational Learning in Five Terrorist Groups* (RAND Corporation, 2005), http://www.rand.org/pubs/monographs/2005/RAND_MG332.pdf

[45] Rohan Gunaratna, *Inside Al Qaeda*, 140-141.

[46] "Anti-terror police under pressure," *Financial Times Information*, July 11, 2007.

[47] *Intelligence and Security Committee Report,* 39.